UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

**EXAMINER'S AMENDMENT**

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with Mr. AASHISH KARKHARIS on May 12, 2008.

3. The applicant has been amended as follow:

In the claims:

Claim 5, line 1, after the words "the method for using a", have been added "partially encrypted" and deleted "Previously Amended", and line 2 after the words " wherein authenticating the " have been added " partially encrypted" and deleted " previously Amended".

***Reasons for allowance***

4. The following is an examiner's statement of reasons for allowance:

In interpreting the claims, in light of the specification and the applicant's arguments filed on April 4, 2008 and November 13, 2007 the examiner finds the claimed invention to be patentably distinct from the prior art of record.

5. Gennaro et al., (5,937,066), teaches a cryptographic key recovery system that operates in two phases. In the first phase, the sender establishes a secret value with the receiver. For each key recovery agent, the sender generates a key-generating value as a one-way function of the secret value and encrypts the key-generating value with a public key of the key recovery agent. In the second phase, performed for a particular cryptographic session, the sender generates for each key recovery agent a key-encrypting key as a one-way function of the corresponding key-generating value and multiply encrypts the session key with the key-encrypting keys of the key recovery agents. The encrypted key-generating values and the multiply encrypted session key are transmitted together with other recovery information in a manner permitting their interception by a party seeking to recover the secret value. To recover the secret value, the party seeking recovery presents the encrypted key-generating values and public recovery information to the key recovery agents, who decrypt the key-generating values, regenerate the key-encrypting keys from the corresponding key-generating values, and provide the regenerated key-encrypting keys to the recovering party. The recovering party uses the key-encrypting keys to recover the secret value. Since the key-generating values cannot be derived from the key-encrypting keys, they may be used over a period spanning multiple cryptographic sessions without requiring new values or new public key encryptions.

6. Jakobsson; Markus Bjorn., (6,687,822), teaches a A method for providing publicly verifiable translation certificates comprising the steps of receiving an input encryption having a first secret key; outputting an output re-encryption of the input encryption, the output re-encryption having a second secret key; and generating a translation certificate that proves the input encryption and the output re-encryption are encryptions of an identical message, wherein the first secret key and the second secret key do not need to be, but are allowed to be, equal. This method and system for generating translation certificates in quorum controlled asymmetric proxy encryptions has uses, including but not limited to, Internet applications and specifically to E-mail systems. The scheme, which can use either an ElGamal encryption, an ElGamal encryption based on Elliptic Curves or an ElGamal related encryption algorithm, leaks no information as long as there is no dishonest quorum of proxy servers and produces a small, publicly verifiable translation certificate, that is independent of the number of prover servers involved in the re-encryption.

7. Menezes et al., (5,473,691), teaches a system of the present invention processes data for communication between first and second computers by linearizing the communications message. The message comprises a linear header portion, an extended header portion, and a message body. The linear header portion identifies the number of message recipients and message types. The extended header contains detailed information about the message recipients, such as recipient name and address. The extended header may also contain message subject information, polling information, and password data. The header information is used by the receiving computer to prepare to process the expected data type. The message body may be transferred in a form that takes

advantage of the data processing capabilities of the first and second computers. The computers may exchange data processing capabilities so that the most efficient transfer form may be selected. The extended header and message body are encoded using a well-known ASN-1 data encoding process. In addition, the message body may be compressed and encrypted. The system may be readily used in facsimile communication where the first and second computers are facsimile machines.

8. However, the prior art of record fails to teach or suggest individually or in combination that teach a method for using a partially encrypted document, comprising: issuing a document usage request for using the partially encrypted document in a session; authenticating the partially encrypted document; receiving authorization to use the partially encrypted document; receiving a session key for the session; receiving a proxy key that delegates decryption to the session; rendering a non-encrypted portion of the partially encrypted document; performing a proxy transformation on the partially rendered, partially
encrypted document using the proxy key; wherein rendering a portion of the partially encrypted document and performing proxy transformation on the rendered portion of the partially encrypted document comprises a combination of performing partial rendering transformations and performing partial decryption transformations; and decrypting the proxy transformed, partially rendered, partially encrypted document using the session key, wherein the proxy key and the session key are used to decrypt the partially encrypted document as part of the session rendering process only, thereby assuring that only rendered images of the decrypted document are available to an end user as set forth in

independent claims 1, 6 and 12. Claims 2-5, 6-9, and 13 are allowed because of the combination of other limitations and the limitation listed above.

9. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Examiner's Amendment".

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tammy T. Nguyen whose telephone number is 571-272-3929. The examiner can normally be reached on Monday - Friday 8:30 - 5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, ***William Vaughn*** can be reached on 571-272-3922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the

automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/T. N./

Patent Examiner, Art Unit 2144

/William C. Vaughn, Jr./

Supervisory Patent Examiner, Art Unit 2144